Regeringen

DECEMBER 2021

National strategi for cyber- og informationssikkerhed

Indhold

Forord

Danmark er en af verdens førende nationer når det gælder digitalisering. Både i privatlivet, på arbejdspladsen og i mødet med det offentlige Danmark er danskernes hverdag digitaliseret.

Digitalisering er en afgørende drivkraft for udviklingen af det danske samfund. For med den teknologiske udvikling følger nye muligheder for økonomisk vækst og øget velfærd. Men med den høje grad af digitalisering følger også en øget sårbarhed over for kriminelle, der forsøger at udnytte sårbarhederne i vores digitale samfund.

Cybertruslen er i dag en af de mest alvorlige trusler mod Danmark. Den er blevet et grundvilkår, som vi alle sammen må agere efter – i vores privatliv, vores arbejdsliv og i samfundet som helhed.

Hver dag er vores myndigheder, virksomheder og borgere mål for cyberangreb i større eller mindre skala. Hackere, kriminelle og fjendtlige efterretningstjenester sætter danskernes digitale sikkerhed under pres.

Regeringen tager denne trussel meget alvorligt.

Vi har i Danmark allerede et godt fundament til at imødegå udfordringerne. Borgerne i Danmark har generelt en stærk digital forståelse, it-sikkerhed har i mange år været et fokusområde i mange virksomheder, og fra offentlig side har årtiers fokuseret indsats for at fremme digitaliseringen i Danmark givet os en veludviklet platform at stå på.

Men den digitale udvikling går stærkt, og nye cyberangrebsformer kommer til i samme hast. Cybertruslen forandrer sig konstant. Derfor er der behov for en styrket indsats, hvis vi skal følge med og være på forkant med udviklingen i trusler og digitale sårbarheder. Derfor lancerer regeringen nu en ny national strategi for cyber- og informationssikkerhed 2022-2024.

Strategien har fokus på såvel stat og kritisk infrastruktur som på borgerne og på erhvervslivet. For ligesom den udefrakommende cybertrussel truer

os alle, kræver det en fælles indsats, hvis vi skal beskytte Danmark mod ondsindet cyberkriminalitet og cyberspionage.

Regeringen og forligspartierne har allerede med udmøntningen af forsvarsforligets cyberreserve styrket Danmarks cyberforsvar med 500 mio. kr. Og i kommuner og regioner arbejdes ligeledes løbende med at styrke cyber- og informations-sikkerheden.

Nu styrkes indsatsen yderligere med den nationale strategi for cyber- og informationssikkerhed, der indeholder en række nye initiativer og binder den samlede indsats sammen. Med strategien udmønter regeringen i alt 270 mio. kr. til 34 nye hovedinitiativer, som ruster os til at holde cybertruslen i skak og bidrager til, at vi i Danmark kan færdes sikkert digitalt – også i fremtiden.

Det trusselsbillede, vi står overfor, ændrer sig konstant og kræver at vi alle – myndigheder, virksomheder og borgere – kontinuerligt deltager og tager aktivt ansvar. Arbejdet med cybersikkerhed er en opgave, som vi aldrig når i mål med. For hackere, kriminelle og cyberspioner udfordrer løbende vores sikkerhed med nye og mere avancerede angrebsmetoder. Med den nationale strategi for cyber- og informationssikkerhed tager vi et vigtigt skridt i retning af en øget fælles indsats og en styrkelse af vores værn mod den cybertrussel, som i dag udgør en af de største trusler mod Danmark og det danske samfund.

/**Regeringen**

En markant og kompleks cybertrussel i konstant forandring

Truslen fra cyberkriminalitet og cyberspionage er i dag meget høj, og den må også forventes at være det i fremtiden. Fremmede stater og kriminelle hackere arbejder systematisk, vedholdende og målrettet på at ramme nøje udvalgte mål i Danmark, og de forsøger løbende at misbruge den fortsatte digitalisering af vores samfund til at spionere, udøve kriminalitet og underminere demokratiske processer – og i sidste ende potentielt at udføre destruktive cyberangreb mod Danmark.

Den digitale infrastruktur er i stigende grad en forudsætning for, at vores samfund fungerer. Men jo flere digitale systemer, vi anvender og kobler sammen, desto flere steder kan vi blive udsat for angreb. Det seneste års cyberangreb mod bl.a. det irske sundhedsvæsen og olie- og fødevareindustrien i USA viser med al tydelighed nogle af de konsekvenser, sådanne angreb kan have for en nations evne og mulighed for at opretholde samfundsvigtige funktioner.

Cyberkriminalitet er i dag en yderst profitabel industri. De kriminelle er dygtige, professionelle og drevet af mulighederne for at tjene penge. De omstiller sig hurtigt, når nye indtjeningsmuligheder opstår, når nye værktøjer udvikles, eller når de ydre omstændigheder ændrer på deres kriminelle forretningsgrundlag.

Samtidig er spionagetruslen fra fremmede staters efterretningsvirksomhed blevet mere markant. Fremmede staters efterretningstjenester anvender teknologiske fremskridt og gør brug af avancerede hackergrupper, der gennem cyberangreb er i stand til at kompromittere og få adgang til it-systemer til at udøve efterretningsvirksomhed mod Danmark. Visse staters efterretningsvirksomhed bliver brugt til at stjæle værdifuld viden fra både Danmark og vores allierede. Angrebene er ofte komplekse, og såvel politikere, embedsfolk og myndigheder som forskningsinstitutioner og virksomheder kan indgå som enten mål eller middel i disse aktiviteter.

Danmark er et attraktivt mål for cyberangreb på grund af vores aktive rolle på den internationale scene, i den øgede globalisering og internationale konkurrence. Digitaliseringen og den generelle åbenhed i samfundet samt et højt teknologisk vidensniveau gør Danmark til et attraktivt mål for cyberangreb, ligesom Danmarks aktive internationale rolle tiltrækker såvel ønsket som uønsket opmærksomhed.

Samtidig står en række nye digitale muligheder som kunstig intelligens, big data, kvanteteknologi og 5G for døren. Dette stiller høje krav til, hvordan vi som samfund håndterer vores beskyttelsesværdige informationer og den digitale infrastruktur, som er så afgørende for opretholdelsen af vores samfundsvigtige funktioner. Ligeledes stiller det krav til de virksomheder, der indgår i forsyningskæderne.

Hver dag angriber cyberkriminelle og spioner Danmark for at afpresse danske virksomheder, myndigheder og borgere, for at stjæle vores forretningshemmeligheder, som sikrer Danmarks velstand, og for at afsløre og udfordre detaljer om vores sikkerheds- og udenrigspolitik til skade for Danmark og danske interesser.

Langt de fleste hackerangreb bliver heldigvis afværget takket være allerede implementerede tekniske sikkerhedsforanstaltninger og opmærksomme myndigheder, virksomheder og borgere. Men det går også galt engang imellem, og der er i dag alt for mange sikkerhedshuller, som kun venter på at blive opdaget af hackere og cyberkriminelle.

For ligesom mange først køber en tyverialarm, efter de har haft indbrud, lykkes mange hackerangreb på grund af overset eller nedprioriteret cybersikkerhed, som først prioriteres, når skaden er sket. Hackerne har langt fra vundet kampen om det digitale domæne, men arbejdet med at gøre Danmark digitalt sikkert er vigtigere og mere presserende end nogensinde.



Digitaliseringen og den generelle åbenhed i samfundet gør Danmark til et attraktivt mål for cyberangreb

Center for Cybersikkerheds hovedvurdering af cybertruslen mod Danmark



Truslen fra cyberkriminalitet: MEGET HØJ



Alle danske myndigheder, virksomheder og borgere er udsat for en vedvarende og aktiv trussel fra cyberkriminelle. Truslen underbygges af de cyberkriminelles evne til at udvikle og omstille sig til nye virkeligheder samt af det specialiserede samarbejde, der foregår på det lukkede internet.



Truslen fra cyberspionage: MEGET HØJ



Center for Cybersikkerhed vurderer, at fremmede stater kan og vil forsøge på at stjæle værdifuld information fra Danmark. Særligt interessante mål på det udenrigs- og sikkerhedspolitiske område er udsat for en vedvarende interesse fra statslige aktører. Konkrete hændelser og løbende angrebsforsøg understreger gang på gang denne vurdering.



Truslen fra destruktive cyberangreb: LAV

Center for Cybersikkerhed vurderer, at truslen fra destruktive cyberangreb mod danske myndigheder og virksomheder er lav. Flere stater har kapaciteten til at udføre destruktive angreb, men det er mindre sandsynligt, at de aktuelt har intentionen om at udføre denne type angreb mod danske mål.



Truslen fra cyberaktivisme: LAV

De mange protester, der har præget 2020, har ikke ført til en stigning i antallet af cyberaktivistiske angreb på verdensplan. Antallet af angreb ligger således på niveau med de seneste år.

Et løft af cyber- og informations-sikkerheden i Danmark

Den hidtidige indsats for et højt cyber- og informationssikkerhedsniveau har øget modenheden på tværs af samfundet. Der er en større bevidsthed om og opmærksomhed på området. Cybersikkerheden er styrket i staten og i seks udpegede samfundskritiske sektorer (energi, sundhed, transport, tele, finans og søfart) med etablering af decentrale cyber- og informationssikkerhedsenheder (DCIS) og målrettede strategier. Derudover skal statslige myndigheder følge den internationale ledelsesstandard ISO 27001, og der er indført en række tekniske minimumskrav i staten, som fastlægger en ramme for ledelsesforankret risikobaseret styring af informationssikkerhed.

Der er også sket en generel styrkelse af kompetencerne hos borgere og virksomheder, hvad angår cyber- og informationssikkerhed.

Samtidig er der i EU et stort fokus på at højne cybersikkerheden bl.a. ved revision af direktiv om sikkerhed i net- og informationssystemer i samfundskritiske sektorer. Det stiller også krav til, at Danmark øger ambitionsniveauet, herunder hvad angår risikostyret ledelsesforankring, implementering af sikkerhedsforanstaltninger og it-beredskab.



NIS-direktivet

Direktiv om sikkerhed i net- og informationssystemer i samfundskritiske sektorer (NIS-direktivet)

EU-direktivet om sikkerhed i net- og informationssystemer i samfundskritiske sektorer (NIS-direktivet) fra 2016 er et væsentligt instrument i at højne cyber- og informationssikkerheden i de samfundsvigtige sektorer i Danmark. I december 2020 fremsatte Kommissionen et forslag til revision af direktivet, hvor der lægges op til at udvide direktivets dækningsområde i bredden og dybden bl.a. i form af nye krav til cybersikkerheden i de omfattede virksomheder og myndigheder samt til medlemsstaternes tilsyn med cybersikkerheden. Formålet er ledelsesforankret risikostyring, implementering af organisatoriske og tekniske foranstaltninger samt styr på beredskabet, der gør organisationer i stand til hændelseshåndtering (før, under og efter) og operativt samarbejde på tværs af organisationer og landegrænser i EU.

Et løft af cybersikkerheden i Danmark kræver en samlet indsats og et fælles ansvar på tværs af samfundet. Staten har ansvaret for at varetage den nationale sikkerhed. Virksomheder og myndigheder har et ansvar for at varetage sikkerheden i egen organisation. Og alle borgere skal have en forståelse for, hvordan egne handlinger kan påvirke egen og andres digitale sikkerhed.

Med den nationale strategi for cyber- og informationssikkerhed 2022-2024 skrues der op for ambitionerne og målsætningerne for et cyber- og informationssikkert Danmark. Regeringen retter med strategien særligt fokus på sikkerheden i den kritiske it-infrastruktur, der understøtter samfundsvigtige funktioner.



Ordforklaring

Samfundsvigtige funktioner
De aktiviteter, varer og tjenesteydelser, som udgør grundlaget for samfundets generelle funktionsdygtighed.

Kritisk infrastruktur
Infrastruktur, herunder systemer, tjenester, processer, netværk og aktiver samt serviceydelser, der er nødvendige for at opretholde eller genoprette samfundsvigtige funktioner.

Kritisk it-infrastruktur
Den delmængde af kritisk infrastruktur, der omfatter den digitale infrastruktur, der er nødvendig for at opretholde eller genoprette samfundsvigtige funktioner.

Samfundskritiske it-systemer
De it-systemer, hvor større driftsforstyrrelser resulterer i væsentlige udfordringer for samfundet som helhed. Utilgængelighed og ustabil drift i it-systemerne kan få markante følger for samfundet og for opretholdelsen af samfundskritiske processer.

En ambitiøs indsats i staten og samfundsvigtige funktioner
Robuste og modstandsdygtige samfundsvigtige funktioner kræver et højt cyber- og informationssikkerhedsniveau i den understøttende kritiske it-infrastruktur. Det kræver en ambitiøs indsats fra både offentlige og private aktører. Strategien udvides fra at omfatte de seks nuværende samfundskritiske sektorer til også at omfatte en bredere kreds af ministerområder med ansvar for samfundsvigtige funktioner, der i væsentlig grad er it-understøttet.

Alle statslige myndigheder skal fortsat efterleve en række minimumskrav til sikkerheden, som vil blive udbygget i strategiperioden. Det samme gælder kravene til ministerområder, der har ansvaret for samfundskritiske it-systemer eller samfundsvigtige funktioner, for hvem der stilles en række yderligere sikkerhedskrav. Det skal samlet set bidrage til, at ministerområder med et særligt ansvar for samfundsvigtige funktioner i Danmark er klædt på til at kunne agere hurtigt og effektivt i tilfælde af en alvorlig cyberhændelse.

Cyber- og informationssikkerhed i staten: Nye krav til statslige myndigheder

Ministerområder (eller dele heraf) med ansvar for samfundsvigtige funktioner



Vil skulle efterleve en række nye krav til organisering af sikkerhedsarbejdet omkring den samfundsvigtige funktion, bl.a. krav om oprettelse af DCIS og udarbejdelse af egen strategi for den samfundsvigtige funktion

Statslige myndigheder med ansvar for samfundskritiske it-systemer



Vil skulle efterleve en række nye myndighedskrav relateret til systemerne, bl.a. nye krav til kontrakt- og leverandørstyring samt skærpede krav om udarbejdelse af beredskabsplaner

Alle statslige myndigheder



Vil fortsat skulle efterleve minimumskrav til bl.a. organisering af sikkerhedsarbejdet, efterlevelse af ISO 27001 og tekniske minimumskrav

Fokus på erhvervslivet
Cyber- og informationssikkerhed skal være en prioritet for alle danske virksomheder, herunder særligt de små og mellemstore virksomheder. Mange SMV'er rammes af cyberangreb, og tendensen er stigende. De ca. 300.000 SMV'er skal have styr på sikkerheden, da et angreb kan have store omkostninger for den enkelte virksomhed, fx gennem tabt omsætning. Det kan i yderste konsekvens betyde, at en virksomhed mister sit forretningsgrundlag og må dreje nøglen om.

Med strategien sætter regeringen fokus på en stærkere og mere sammenhængende SMV-indsats. Ved at styrke det digitale sikkerhedsniveau hos SMV'erne sikrer vi et Danmark, der fortsat er konkurrencedygtigt og har gode vækstvilkår.



Vækst for virksomheder

Vækstvilkår for cyber- og informationssikkerhedsøkosystemet i Danmark

Et styrket dansk cyberøkosystem kan både skabe vækst i cybersikkerhedsindustrien og styrke det generelle cybersikkerhedsniveau i Danmark på tværs af myndigheder og virksomheder med et stærkere leverandørudbud, der forstår det danske marked og dets behov. En stærk dansk cybersikkerhedsindustri er central for at kunne bidrage til europæisk strategisk autonomi på området. Det fordrer stærk videndeling og netværksdannelse. EU har besluttet, at der i de enkelte medlemslande skal oprettes nationale koordinationscentre for cybersikkerhed, der skal understøtte cybersikkerhedsindustrien og samarbejde med det europæiske kompetencecenter (ECCC).

Borgerne
Danmark er et af de lande i verden, hvor digitaliseringen af hverdagen er længst fremme. Det at kunne begå sig og færdes trygt i en digital hverdag kræver høj tillid fra borgerne til de offentlige it-systemer og -løsninger.

Som borger kan det være vanskeligt at navigere i et trusselsbillede i konstant udvikling, hvor nye angrebsmetoder og tilgange konstant udvikles. Den stigende it-kriminalitet og digitale svindel rettet mod borgere tilsiger et behov for en sikker digital adfærd og en øget viden om cyber- og informationssikkerhed.

De danske borgere skal derfor være klædt på til at agere i en digital hverdag og anvende de digitale services og produkter på sikker vis. Med strategien sættes der ind for at løfte vidensniveauet og kompetencerne inden for digital adfærd og sikkerhed hos borgerne med tiltag, der motiverer og engagerer, skaber øget kendskab og interesse samt udvikler gode og sikre digitale vaner hos borgerne.



Hotline

Hotline ved identitetstyveri

Regeringen har taget initiativ til en ny hotline til borgere til hjælp ved digital identitetstyveri, der blev lanceret juni 2021 i Digitaliseringsstyrelsen. Hotlinen har døgnåbent året rundt og danner rammen for ét samlet kontaktpunkt med rådgivning for borgere, der enten har været udsat for eller har mistanke om digitalt identitetstyveri.

Strategiske målsætninger

Med strategien sætter regeringen fire strategiske målsætninger, der sætter rammen for udviklingen mod et stærkere og mere sikkert digitalt Danmark.

Regeringen ønsker



1. Robust beskyttelse af de samfundsvigtige funktioner

- Vi skal kunne opretholde samfundsvigtige funktioner og økonomisk aktivitet i en krisesituation, hvor kritisk it-infrastruktur sættes ud af kraft i kortere eller længere tid.
- Statslige myndigheder og virksomheder skal have et tilfredsstillende sikkerhedsniveau og skal med kort varsel være i stand til at agere i tilfælde af alvorlige cyberhændelser.



2. Øget kompetenceniveau og ledelsesforankring

- Cyber- og informationssikkerhed skal være forankret i topledelsen, og kompetencerne skal styrkes. Det gælder ift. overblik over aktiver, sårbarheder og kendskab til potentielle trusler.
- Borgere, virksomheder og statslige myndigheder skal vide, hvordan de beskytter sig og færdes sikkert digitalt.
- Efterspørgslen på cyber- og informationssikkerhedskompetencer skal imødekommes ved at uddanne flere specialister og opbygge stærkere kapacitet på tværs af samfundet.



3. Styrkelse af det offentligt-private samarbejde

- Statslige myndigheder og virksomheder skal have et stærkere samarbejde og være bedre til at dele viden og erfaringer om trusler og hændelser.
- Statslige myndigheder og virksomheder skal være understøttet med højt specialiseret rådgivning fra centralt hold.



4. Aktiv deltagelse i den internationale kamp mod cybertruslen

- Det internationale samarbejde i EU, FN, NATO og ligesindede lande skal styrkes – det skal være besværligt og have konsekvenser at udføre cyberangreb mod Danmark.
- Danmark skal aktivt bidrage til at sikre et åbent, sikkert og troværdigt internet og beskytte kritisk it-infrastruktur.

1

Robust beskyttelse af de samfunds-vigtige funktioner

- Vi skal kunne opretholde samfundsvigtige funktioner og økonomisk aktivitet i en krisesituation, hvor kritisk it-infrastruktur sættes ud af kraft i kortere eller længere tid.

- Statslige myndigheder og virksomheder skal have et tilfredsstillende sikkerhedsniveau og skal med kort varsel være i stand til at agere i tilfælde af alvorlige cyberhændelser.



Modenheden i arbejdet med cyber- og informationssikkerhed er generelt stigende i Danmark, også hos de statslige myndigheder. Der er dog fortsat en række centrale udfordringer, herunder manglende forståelse for cybertruslen samt komplekse it-systemer, der gør arbejdet svært.

Samfundsvigtige funktioner som energiforsyning, jernbanetransport og forskning er i stigende grad digitaliseret, hvilket kræver fokus på den kritiske it-infrastruktur, der understøtter disse. Der er behov for bedre overblik over den kritiske it-infrastruktur og afhængigheder mellem de it-systemer, der understøtter samfundsvigtige funktioner. Derfor skal ministerområder med ansvar for samfundsvigtige funktioner have en klar plan for arbejdet med cybersikkerhed og kunne indgå i det operative samarbejde.

Mange statslige myndigheder mangler basale tekniske sikkerhedsforanstaltninger og efterlever fortsat ikke de fastsatte tekniske minimumskrav, ligesom sikkerhedsniveauet for en stor del af de samfundskritiske it-systemer i staten i dag ikke er tilstrækkeligt. Siden 2016 har de statslige myndigheder været forpligtet til at følge den internationale sikkerhedsstandard ISO 27001, der fastsætter bedste praksis for styring af informationssikkerhed. Over en tredjedel af myndighederne er endnu ikke i mål med at implementere standarden.

Robuste og modstandsdygtige samfundsvigtige funktioner forudsætter også, at danske virksomheder har en tilstrækkelig digital sikkerhed, og at politiet har kapacitet til at forebygge og efterforske it-relateret økonomisk kriminalitet.

Men i dag har 40 pct. af de danske små og mellemstore virksomheder et digitalt sikkerhedsniveau, der er utilstrækkeligt i forhold til deres risikoprofil, og mange virksomheder mangler helt grundlæggende tiltag i deres digitale sikkerhed[1]. Der er derfor behov for at styrke den digitale robusthed i de danske virksomheder, herunder særligt de små og mellemstore virksomheder.

Anmeldelser af økonomisk it-relateret kriminalitet er steget markant de seneste år. Politiets Landsdækkende Center for it-relateret Økonomisk Kriminalitet (LCIK) har siden sin oprettelse i december 2018 modtaget 70.000 anmeldelser om økonomisk it-kriminalitet[2]. Dette understreger behovet for en styrket forebyggelses- og efterforskningsindsats.

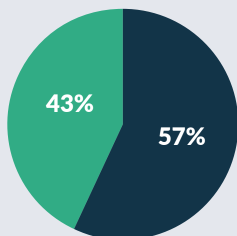
Med strategien igangsættes en række strategiske indsatser, som skal styrke sikkerheden i de samfundsvigtige funktioner samt sikre, at myndigheder og virksomheder har et tilstrækkeligt sikkerhedsniveau.

1 Digital sikkerhed i danske SMV'er 2021

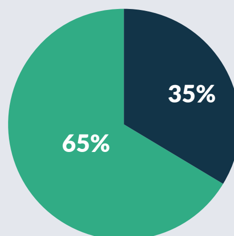
2 Landsdækkende Center for It-relateret Kriminalitet

De statslige myndigheders sikkerhedsniveau er flere steder utilstrækkeligt

Status på ISO 27001-implementering



Status på de tekniske minimumskrav



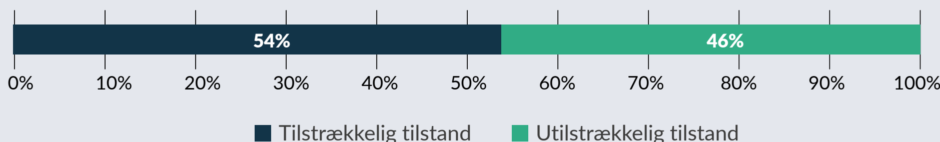
■ Implementeret ■ Ikke implementeret

■ Implementeret ■ Ikke implementeret

Statslige myndigheder er forpligtet til at følge sikkerhedsstandarden ISO 27001 og implementere 20 tekniske minimumskrav. Kun 57 pct. har opnået fuld implementering af ISO 27001, og kun 35 pct. efterlever alle 20 krav.

Kilde: Digitaliseringsstyrelsen

For mange samfundskritiske it-systemer i staten er i utilstrækkelig tilstand



■ Tilstrækkelig tilstand ■ Utilstrækkelig tilstand

46 pct. af de samfundskritiske it-systemer i staten er i utilstrækkelig tilstand. For en stor andel af it-systemerne er årsagen utilstrækkeligheder med den tekniske tilstand og/eller et utilstrækkeligt sikkerhedsniveau.

Kilde: Digitaliseringsstyrelsen

Virksomhederne har ikke implementeret basale sikkerhedstiltag

Sikkerhedstiltag mangler

24%

af de små og mellemstore virksomheder har ikke implementeret de to grundlæggende sikkerhedstiltag back-up og automatisk opdatering af software.

Kilde: Digital sikkerhed i Danske SMV'er 2021

Utilstrækkeligt sikkerhedsniveau

40%

af de små og mellemstore virksomheder har et utilstrækkeligt digitalt sikkerhedsniveau i forhold til deres risikoprofil.

Kilde: Digital sikkerhed i Danske SMV'er 2021



Strategiske indsatser

- Sikkerheden og samarbejdet omkring samfundsvigtige funktioner og samfundskritiske it-systemer styrkes med nye krav til organiseringen af sikkerhedsarbejdet, bl.a. krav om delstrategi og decentrale cyber- og informationssikkerhedsenheder.
- Der stilles skærpede sikkerhedskrav til styringen af statslige samfundskritiske it-systemer, der skal sørge for, at sikkerheden i og omkring it-systemerne har det rette ledelsesmæssige fokus.
- Sikkerheden hos de statslige myndigheder styrkes ved at indføre nye tekniske minimumskrav. Samtidig styrkes rådgivningsindsatsen om sikkerhedsstandarden ISO 27001 med henblik på, at alle statslige myndigheder implementerer den fuldt ud.
- Der opbygges et stærkere teknisk bolværk i staten via nye fælles tekniske løsninger, der skal beskytte statslige ansatte mod phishing og malware. Der etableres fælles statslig logning som et it-sikkerhedsskjold, der skal give bedre mulighed for at identificere og imødegå trusler. Statslige myndigheders muligheder for indrapportering og deling af trusler med hinanden styrkes ligeledes.
- Der skabes et bedre overblik af kritisk it-infrastruktur, der understøtter samfundsvigtige funktioner.
- Viden om og opmærksomhed på digital sikkerhed blandt virksomhedernes ledelser, medarbejdere og rådgivere, fx revisorer og bankrådgivere, øges. Derudover får virksomheder adgang til effektive og brugervenlige værktøjer, som de kan bruge til at løfte deres digitale sikkerhedsniveau, særligt målrettet SMV-segmentet.
- Politiets indsats mod it-relateret kriminalitet styrkes ved at udvide kapaciteten til bagudrettet efterforskning og disruption af it-relateret kriminalitet samt mulighed for, at politiet kan rykke ud til virksomheder ved cyberangreb.

2

Øget kompetence-niveau og ledelses-forankring

- Cyber- og informationssikkerhed skal være forankret i topledelsen, og kompetencerne skal styrkes. Det gælder ift. overblik over aktiver, sårbarheder og kendskab til potentielle trusler.

- Borgere, virksomheder og statslige myndigheder skal vide, hvordan de beskytter sig og færdes sikkert digitalt, og der skal uddannes flere specialister med cyber- og informations-sikkerhedskompetencer.



Danskerne bliver i stadigt stigende grad mere bevidste om cyber- og informationssikkerhed[3]. Men der ligger en udfordring i at få omsat bevidsthed til viden, kompetencer og handling, der sikrer et løft af cyber- og informationssikkerheden.

Cybersikkerhed kræver topledelsesforankring, så sikkerhed bliver en mere integreret del af ledelsesopgaven, og det kræver besiddelsen af de rette kompetencer.

Men særligt de små og mellemstore virksomheder besidder ikke de kompetencer og ressourcer, der skal til for at implementere passende sikkerhedsforanstaltninger. Der ligger dog en tværgående udfordring i både at rekruttere såvel som fastholde relevante kompetencer inden for cyber- og informationssikkerhedsområdet. For efterspørgslen på cyber- og informationssikkerhedskompetencer er stor, men både myndigheder og virksomheder oplever, at det er vanskeligt at skaffe de rette profiler til opgaverne. Der er derfor behov for at styrke udbuddet af kompetencer, hvis sikkerheden skal løftes bredt set.

Endelig er der også behov for at indsatser understøtter bedre kompetencer blandt den danske befolkning. Borgerne skal kunne begå sig sikkert i en digital hverdag – det gælder både børn, unge og voksne, så de i videst mulig omfang undgår at blive ofre for it-kriminalitet eller digital svindel.

For at sikre et højt cyber- og informationssikkerhedsniveau på tværs af samfundet igangsættes der med strategien en række indsatser med fokus på at øge kompetencer og sikre ledelsesforankring. Der igangsættes ligeledes indsatser rettet mod børn, unge og voksne gennem uddannelse, så den danske befolkning bliver mere digitalt veluddannet.



Undersøgelsen *Danskernes informationssikkerhed* 2020 har bl.a. vist, at viden om cyber- og informationssikkerhed ikke er tilstrækkelig udbredt i befolkningen og blandt medarbejdere i både statslige myndigheder og virksomheder

3 Danskernes informationssikkerhed 2020

Mangel på ledelsesforankring og kompetencer



22%

af de virksomheder og myndigheder, der har forsøgt at rekruttere informationssikkerheds-arbejdskraft, har enten ikke kunne ansætte eller har måtte ansætte en profil, som ikke havde alle de ønskede kompetencer.

Kilde: Arbejdsmarkedet for informationssikkerheds-kompetencer i Danmark

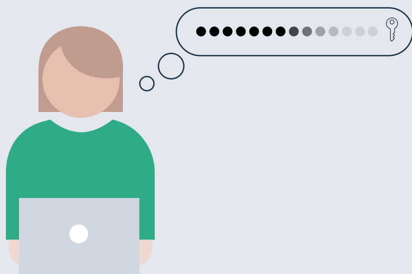


26%

af de danske SMV'er træffer beslutninger om virksomhedens arbejde med digital sikkerhed, hvor ledelsen kun i nogen eller mindre grad er involveret.

Kilde: Digital sikkerhed i Danske SMV'er 2021

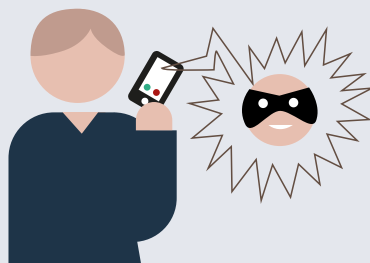
Borgerne mangler viden om cyber- og informationssikkerhed



16%

af borgerne efterlever anbefalingen om at have et kode-ord på mere end 12 tegn og ikke genbruges flere steder.

Kilde: Danskernes informationssikkerhed 2020



21%

af danskerne har i 2020 oplevet fupopkald.

Kilde: Danskernes informationssikkerhed 2020



Strategiske indsatser

- Forankring og prioritering af cyber- og informationssikkerhed i alle ledelseslag sikres ved at styrke viden, awareness og adfærd for topledere og ledere i staten via øgede krav og forventninger samt nye kompetenceindsatser.
- De statslige ansattes kompetencer inden for cyber- og informationssikkerhed styrkes med nye kursusindsatser gennem bl.a. Statens Digitaliseringsakademi målrettet både specialister og generalister.
- Det sikres, at børn, unge og voksne rustes til at begå sig sikkert digitalt ved at gennemføre en bred indsats på undervisnings- og uddannelsesområdet, bl.a. ved at udbrede inspirationsmateriale og øge awareness i alle uddannelsesled.
- Samfundets adgang til kompetencer inden for cyber- og informationssikkerhed styrkes gennem de videregående uddannelser bl.a. inden for ordinære uddannelser og videregående voksen-, efter- og videreuddannelse.
- Cyber- og informationssikkerheden blandt borgere, virksomheder og statslige myndigheder løftes ved at styrke informationsindsatsen rettet mod målgrupperne gennem videreudvikling af informationsportalen Sikkerdigital.dk.

3

Styrkelse af det offentligt-private samarbejde

- Statslige myndigheder og virksomheder skal have et stærkere samarbejde og være bedre til at dele viden og erfaringer om trusler og hændelser.

- Statslige myndigheder og virksomheder skal være understøttet med højt specialiseret rådgivning fra centralt hold.



Evnen til at dele viden og erfaringer om cyber- og informationssikkerhedshændelser er afgørende for at opnå et højt cyber- og informationssikkerhedsniveau. Der er derfor behov for, at samarbejdet på tværs af sektorer styrkes, så vi kan blive endnu bedre til at dele viden på tværs og lære af hinanden. Statslige myndigheder skal også være bedre til at anvende data fra indberetninger til at formidle viden om trusler og sårbarheder.

Der er stor efterspørgsel på rådgivning fra centralt hold, og der er brug for at styrke kapaciteten og den samlede rådgivningsindsats rettet mod statslige myndigheder for at imødekomme efterspørgslen.

Også borgere og virksomheder, der udsættes for eksempelvis phishingforsøg og hacking, kan i dag have svært ved at vide, hvor de skal henvende sig, og hvilken rådgivning de har brug for. Borgere kan i dag få rådgivning fra hotlinen for identitetstyveri, men der er behov for bredere hjælp og rådgivning for både virksomheder og borgere, herunder også om grundlæggende cyber- og informationssikkerhed.

I erhvervslivet er der behov for et stærkere og tættere samarbejde. Generelt er indsatserne rettet mod SMV'erne fortsat fragmenterede, og de har ofte kun karakter af awareness- og vejledningsindsatser. Skal cyber- og informationssikkerheden løftes hos hele erhvervslivet, er det afgørende, at den samlede virksomhedsindsats for cyber- og informationssikkerhed er koordineret og sammenhængende. Der er behov for konkrete værktøjer, så de danske virksomheder fortsat er konkurrencedygtige.

Gennem en række konkrete indsatser i strategien styrker regeringen det offentligt-private samarbejde om cyber- og informationssikkerhed. Indsatserne sikrer bedre muligheder for videns- og erfaringsudveksling, styrker rådgivningsindsatsen mod både myndigheder, virksomheder og borgere samt bidrager til danske virksomheders konkurrencedygtighed via konkrete værktøjer.

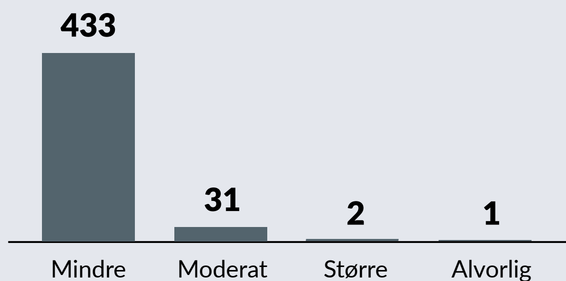
Et forventet mørketal



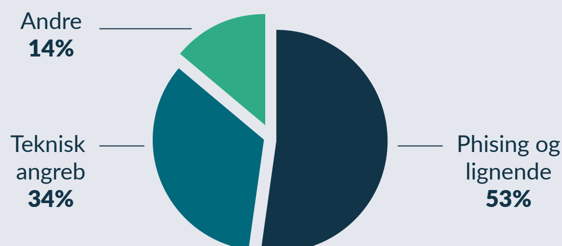
Da ikke alle virksomheder, borgere og myndigheder formodes at indberette alle hændelser, forventes der at være et betydeligt mørketal af it-sikkerhedshændelser.

Hændelsesstørrelse og angrebsveje varierer

I 2020 håndterede Center for Cybersikkerhed 467 sikkerhedshændelser, som har haft effekt på de berørte organisationer.



Identificerede angrebsveje 2020





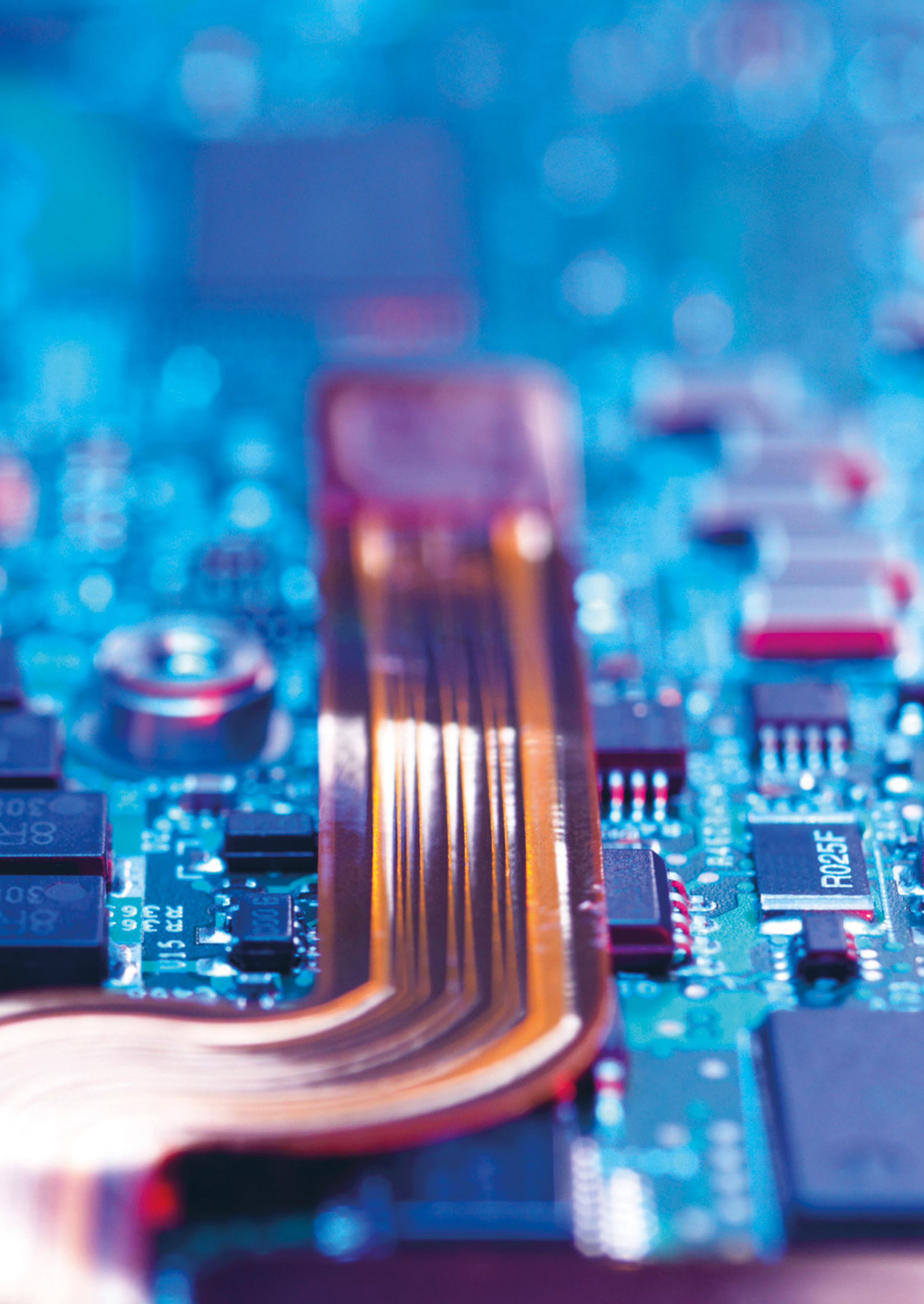
Strategiske indsatser

- Der tilbydes bedre hjælp til borgere og virksomheder via en cyberhotline, hvor det er muligt at søge rådgivning og vejledning, hvis man har været udsat for cyber- eller it-kriminalitet, eller har mistanke herom. Cyberhotlinen tænkes sammen med den allerede etablerede hotline ved identitetstyveri.
- Den situationsbestemte rådgivning til statslige myndigheder styrkes. Den centrale rådgivningskapacitet hos Center for Cybersikkerhed, der leverer råd og vejledning inden for styring af cyber- og informationssikkerhed, styrkes.
- Erfaringsudveksling om og indsigt i cyber- og informationssikkerhedshændelser samt datadeling mellem statslige myndigheder og virksomheder styrkes med henblik på bedre at kunne rådgive, varsle og forebygge hændelser.
- Fokus på SMV-segmentet øges, så viden og erfaringer bringes mere i spil. Der oprettes en cybersikkerhedsenhed for SMV'er, der får til opgave at gennemføre en samlet og koordineret indsats for at styrke videndeling og cybersikkerhedsniveauet i SMV'erne. Enheden skal bl.a. være med til at facilitere og igangsætte nye offentligt-private initiativer, der skal bidrage til en styrkelse af SMV'ernes cybersikkerhed.
- Samarbejde og koordinationen mellem statslige myndigheder om beskyttelse og sikring af informationer på tværs af statslige myndigheder styrkes via rådgivningstilbud.

Offentligt-privat samarbejde om cyber- og informationssikkerhed

Cybersikkerhedsrådet rådgiver regeringen om, hvordan den digitale sikkerhed styrkes og sikrer videndeling mellem myndigheder, erhvervsliv og forskningsverden. Rådet har i sin første periode bl.a. bidraget til udvikling af den nationale cyber- og informationssikkerhedsstrategi 2022-2024, afholdt en række webinarer og bidraget til den nationale cybersikkerhedsmåned. Rådet har også være inddraget i udviklingen af SmitteStop app'en og det digitale coronapas.

Virksomhedsforum for Digital Sikkerhed understøtter regeringens arbejde med at fremme og styrke det danske erhvervslivs digitale sikkerhedsniveau. Forummet bidrager til et generelt løft af den digitale sikkerhed i dansk erhvervsliv, ved at komme med anbefalinger til regeringen og erhvervslivet og fungere som strategisk partner for regeringen i udviklingen og implementeringen af konkrete indsatser. Herunder den kommende cybersikkerhedsenhed for SMV'er.


R025F

4

Aktiv deltagelse i den internationale kamp mod cyber-truslen

- Det internationale samarbejde i EU, FN, NATO og med ligesindede lande skal styrkes – det skal være besværligt og have konsekvenser at udføre cyberangreb mod Danmark.

- Danmark skal aktivt bidrage til at sikre et åbent, sikkert og troværdigt internet samt beskytte kritisk it-infrastruktur.



Det digitale domæne er en integreret del af international politik i det 21. århundrede, og det er en af frontlinjerne i forsvaret for den regelbaserede internationale orden, som også her er under pres.

Danmark udsættes løbende for angreb iværksat af andre stater. Ondsindede aktører ønsker at stjæle værdifulde informationer, højteknologisk viden eller indsætte malware, der senere kan bruges i tilspidsede situationer. Selvom Danmark kan gøre meget, er der behov for styrket internationalt samarbejde i de organisationer, der kan sætte normer og standarder for cyberspace, hvis de bagvedliggende årsager til cyberangreb skal bekæmpes.

Visse autoritære stater arbejder aktivt på at underminere folkerettens anvendelse i cyberspace og øge kontrollen over internettet, mens de samtidig udnytter den samme globale it-infrastruktur til cyberangreb, påvirkningskampagner og aggressiv cyberspionage. Når der ikke eksisterer en regelbaseret international orden i cyberspace, udviskes grænsen mellem krig og fred. Det gør det svært for Danmark og vores allierede at afværge og svare igen på ondsindet cyberaktivitet. Og det udfordrer vores sikkerhed, tryghed og økonomiske fremgang. Der er derfor behov for at kunne stille kriminelle aktører til ansvar, og der er ligeledes behov for at kunne afskrække og imødegå ondsindedes cyberangreb.

De multinationale cybersikkerhedsvirksomheder er ofte de første til at afsløre og reagere på cyberangreb. Og tech- og cybersikkerhedsvirksomheder er derfor væsentlige aktører, når stabilitet, orden og spilleregler i cyberspace skal udvikles og opretholdes. Der er derfor behov for at forbedre samarbejdet mellem stater og private virksomheder på strategisk og politisk niveau samt at afklare ansvars- og arbejdsfordelingen, når konkrete cyberhændelser skal håndteres.

For at imødekomme de udfordringer, men også muligheder, der findes på den internationale cyber- og informationssikkerhedsscene igangsættes der med strategien en række indsatser, der skal styrke Danmarks internationale profil, bygge stærkere broer til den internationale tech- og cybersikkerhedsindustri samt gøre det dyrt og kostbart at udøve cyberangreb og -spionage mod Danmark og vores allierede.

Stort fokus på cybersikkerhed i EU med følgende initiativer

- Etablering af en cyberdiplomatisk værktøjskasse, der danner grundlaget for, at EU i stigende grad påtaler cybertruslen, og hvor der er vedtaget sanktioner mod hackere fra Rusland, Kina og Nordkorea.
- Beslutning om oprettelse af Det Europæiske Industri-, Teknologi- og Forsknings-kompetencecenter for Cybersikkerhed (ECCC) og Netværket af Nationale Koordinations-centre, der bl.a. skal øge den europæiske cybersikkerhedsindustris konkurrenceevne og robusthed og gøre cybersikkerhed til en konkurrencemæssig fordel for virksomheder i EU.
- Revision af NIS-direktivet, der sætter yderligere fokus på cybersikkerhed i de samfundsvigtige sektorer og leverandører til disse sektorer.
- Revision af direktiver for bl.a. produkter og radioudstyr, så de inkluderer cybersikkerhed.
- Prioritering af cybersikkerhed i de europæiske støtteordninger Digital Europe og Horizon Europe, bl.a. til etablering af grænseoverskridende samarbejde mellem industri, forskningsinstitutioner og statslige myndigheder.
- Lancering af EU's strategi for cybersikkerhed, bl.a. med fokus på at skabe kollektiv resiliens i Europa

Europæisk ramme for certificering af cybersikkerhed

Øget digitalisering af alt fra tandbørster til biler, øget brug af internet samt opbevaring af data og systemer i skyen betyder øget risiko for cyberangreb. Det er en risiko, der er svær for både borgere og virksomheder at forstå og beskytte sig tilstrækkeligt imod. For at styrke cybersikkerheden, og det indre digitale marked, har EU vedtaget en forordning, der gør det muligt at certificere cybersikkerheden i produkter, tjenester og processer. Derved vil borgere og virksomheder bedre kunne orientere sig i hvilke produkter og tjenester, der lever op til relevante sikkerhedskrav.



Strategiske indsatser

- Danmarks indsats i det internationale samarbejde for et åbent, sikkert og troværdigt internet styrkes gennem øget engagement i EU, NATO og FN.
- Danmarks position og profil i det internationale cyber-samarbejde styrkes med henblik på at styrke muligheden for diplomatiske modsvar, herunder sanktioner samt arbejde for aktivt forsvar igennem brug af den offensive cyberkapacitet.
- Afskrækkelsen af cyberangreb styrkes ved at hæve omkost-ningerne for at angribe Danmark, vores allierede eller vores nære samarbejdspartnere i cyberspace, herunder ved at styrke Danmarks bidrag til at afsløre, afskrække og retsforfølge individer, aktører og organisationer, der misbruger digitale netværk til at stjæle og spionere mod danske borgere, virksomheder og statslige myndigheder.
- Bedre eksportkontrol med digitale produkter fra danske virksomheder og hjælp til erhvervslivet med effektivt at indefryse kriminelles økonomiske midler.
- Samarbejdet med den multinationale tech-industri, tænketanke og academia om imødegåelse af cyberangreb og andre hybride trusler styrkes gennem det teknologiske diplomati og den direkte kanal til techvirksomhedernes hovedsæder.

Governance

Ansvar og roller ved myndigheders arbejde med cyber- og informationssikkerhed

Arbejdet med cyber- og informationssikkerhed er baseret på sektoransvarsprincippet. Det betyder, at den myndighed, der har ansvaret for en opgave til dagligt, bevarer ansvaret under en hændelse. Det gælder både i det daglige beredskab, under hændelser og ved genopretning efter hændelser.

Hændelse inden for en sektor
Den enhed (myndighed, virksomhed og organisation), der har ansvaret for en opgave til daglig, har fortsat ansvaret, når der opstår en cyberhændelse. Enheden skal sikre, at den i den forbindelse får den aftalte bistand fra eventuelle driftsleverandører. Derudover kan enheden få bistand fra de decentrale cybersikkerhedsenheder. Det er enhedens ansvar at aktivere denne bistand, forestå den indledende hændelseshåndtering og – afhængigt af hændelsens omfang – at anmelde til politiet samt indberette til kompetente myndigheder og Center for Cybersikkerhed. Det er ligeledes den ansvarlige myndighed, virksomhed eller organisation, der som udgangspunkt varetager evt. ekstern kommunikation om hændelsen.

Større, tværgående hændelser
Ved større cyberhændelser, der påvirker flere sektorer, kan National Operativ Stab (NOST), der er forankret i Rigspolitiet, og hvor bl.a. PET og FE/Center for Cybersikkerhed er faste medlemmer, aktiveres.



Sektor-ansvars-princip

Sektoransvarsprincippet indebærer bl.a., at:

1. Alle ministre skal sikre et forsvarligt beredskab inden for eget ressort.
2. Sektoransvaret omfatter alle kritiske funktioner og opgaver, som er pålagt lovgivningsmæssigt, politisk eller administrativt.
3. Myndighedernes beredskabsplanlægning skal bygge på en løbende og systematisk risikovurderingsproces, som er forankret i ledelsen.
4. Myndighederne skal løbende overvåge risikobilledet inden for egen sektor.

Sektoransvarsprincippet indebærer, at det er de sektoransvarlige myndigheders ansvar at håndtere hændelsen og dens følger. De sektoransvarlige myndigheder skal desuden sikre et overblik over hændelsens omfang og rapportere dette til relevante myndigheder, herunder Center for Cybersikkerhed samt NOST, hvis denne er etableret, ligesom det er de berørte virksomheder og organisationers ansvar at håndtere hændelsen og dens følger. Afhængigt af hændelsens omfang og karakter kan Center for Cybersikkerhed i den forbindelse assistere de ramte enheder med imødegåelsen af hændelsen. Center for Cybersikkerhed kan således foretage tekniske undersøgelser af cyberangreb med henblik på dels at stoppe den enkelte hændelse og dels at klarlægge eventuelle angrebsmetoder eller sårbarheder, således at samfundets beskyttelse mod tilsvarende situationer kan styrkes. Disse undersøgelser udføres i et tæt samarbejde med den udsatte enhed.

Ved langt de fleste større cyberangreb vil der være behov for både efterforskning og it-sikkerhedstekniske undersøgelser. Der er derfor etableret et tæt samarbejde mellem politiet (herunder PET) og Center for Cybersikkerhed, som indebærer, at der sker en gensidig orientering ved større cyberhændelser, herunder forsætlige angreb, ligesom der ofte vil være et operativt samarbejde i forbindelse med konkrete hændelser.

Kommunikation

Ekstern kommunikation ved mindre hændelser, der ikke berører flere sektorer, håndteres som udgangspunkt af den ansvarlige myndighed, virksomhed eller organisation. Kommunikation om cybertrusler og det aktuelle situationsbillede samt krisekommunikation i forbindelse med cyberhændelser i øvrigt varetages af Center for Cybersikkerhed i samarbejde med den relevante sektoransvarlige myndighed.

I tilfælde af en større, tværgående hændelse vil der skulle ske en koordination af kommunikationen. Via myndighedssamarbejdet inden for NOST koordinerer Det Centrale Operative Kommunikationsberedskab (DCOK) kommunikationen. DCOK har således til opgave at sikre hurtig videregivelse af relevante og koordinerende informationer til offentligheden, herunder medierne. DCOK har endvidere til opgave – om fornødent – at etablere enheder, hvor borgere kan få yderligere oplysninger vedrørende konkrete hændelser.

Myndigheder med et tværgående ansvar for cyber- og informationssikkerhed

Myndighedernes arbejde med cybersikkerhed understøttes af bistand, information, vejledning og rådgivning fra myndigheder med en tværgående og koordinerende funktion på området. Det er myndighedernes ansvar aktivt at efterspørge den bistand, der vurderes relevant.

Myndigheder, der leverer information, rådgivning og vejledning på cyber- og informationssikkerhedsområdet

1. Center for Cybersikkerhed er national it-sikkerhedsmyndighed og varetager en række opgaver af forebyggende og afhjælpende karakter, herunder bl.a. rådgivning. CFCS' netsikkerhedstjeneste kan bidrage til at opdage og varsle om avancerede cyberangreb hos tilsluttede myndigheder og virksomheder. CFCS varsler relevante myndigheder og virksomheder om konkrete cybertrusler, ligesom centeret udarbejder nationale og sektorspecifikke situationsbilleder og trusselsvurderinger.

2. Politiet har til opgave at forebygge og efterforske it-relateret kriminalitet og bringe kriminalitet til ophør. Politiet har desuden det koordinerende ansvar ved større, tværgående hændelser.

3. PET er national sikkerhedsmyndighed og yder bl.a. rådgivning og bistand til offentlige myndigheder og private i sikkerhedsspørgsmål, herunder fysisk sikring, den menneskelige faktor i informationssikkerhed samt håndtering og opbevaring af dokumenter med udgangspunkt i sikkerhedscirkulæret.

4. Digitaliseringsstyrelsen understøtter informationssikkerheden i den offentlige sektor, herunder gennem vejledning om ISO 27001 og fastsættelse af krav til statslige myndigheder bl.a. som led i den statslige it-porteføljestyring. Derudover varetager Digitaliseringsstyrelsen en række borgerrettede informationsopgaver, herunder Sikkerdigital.dk og hotline ved identitetstyveri samt har ansvaret for at koordinere implementeringen af strategien i samarbejde med Forsvarsministeriet.

5. Erhvervsstyrelsen har til opgave at udarbejde og tilbyde viden, vejledning og værktøjer og koordinere indsatser, der har til formål at styrke den digitale sikkerhed i det brede erhvervsliv, særligt i SMV'erne.



Appendix

Initiativer



Robust beskyttelse af de samfundsvigtige funktioner

1.1 Styrket sikkerhed omkring samfundsvigtige funktioner
1.2 De samfundskritiske it-systemer i staten skal være mere sikre
1.3 Bedre sikkerhed via ISO-implementering og nye minimumskrav til de statslige myndigheder
1.4 Større fokus på it-sikkerhed ved offentlige it-indkøb og udbud
1.5 Fælles tekniske løsninger
1.6 Styrket digital robusthed og digital ledelsesforankring i SMV'erne
1.7 Styrkelse af politiets indsats mod it-kriminalitet
1.8 Øget webpatruljering
1.9 Genopretning af data og samfundskritiske it-systemer i staten
1.10 Hjemmel til at imødegå brede og forstyrrende destruktive cyberangreb
1.11 Udvidet analyse af national kritisk it-infrastruktur
1.12 Statslig CVD-politik
1.13 Styrket akkreditering og tekniske sikkerhedseftersyn
1.14 Fokus på internetudbyderes mulighed for at blokere ondsindede domæner
1.15 Alternativ til satellitbaseret tidsstyring
1.16 Styrkelse af udenlandske statsborgeres førstegangsregistrering i CPR



Øget kompetenceniveau og ledelsesforankring

2.1 Styrket indsats i forhold til viden, awareness og adfærd for topledere og ledere i staten
2.2 Statslige ansatte skal have bedre kompetencer inden for cyber- og informationssikkerhed
2.3 Kompetencer i cybersikkerhed for børn, unge og voksne
2.4 Kompetenceopbygning inden for cyber- og informationssikkerhed gennem de videregående uddannelser
2.5 Videndeling og cyber- og informationssikkerhed på forsknings- og uddannelsesområdet
2.6 Styrket informationsindsats over for borgere, myndigheder og virksomheder samt styrkelse af informationsportalen Sikkerdigital.dk



Styrkelse af det offentligt-private samarbejde

3.1 Bedre hjælp til borgere og virksomheder via en cyberhotline
3.2 Styrket central rådgivningskapacitet
3.3 Etablering af en cybersikkerhedsenhed for SMV'er
3.4 Styrket erfaringsudveksling om og indsigt i cyber- og informationssikkerhedshændelser
3.5 Styrket efterforskningskapacitet til cyberspionage
3.6 Et styrket værn om statens informationer
3.7 Styrket sikkerhedstilsyn med systemleverandører og databehandlere



Aktiv deltagelse i den internationale kamp mod cybertruslen

4.1 Styrket bidrag til en regelbaseret international orden
4.2 Diplomatiske modsvar
4.3 Styrket kapacitet til at kunne imødegå statslige og ikke-statslige aktørers cyberangreb
4.4 Styrket afskrækkelse af cyberangreb
4.5 Styrket kontrol med spredning af cyberprodukter og indefrysning af økonomiske midler



Robust beskyttelse af de samfundsvigtige funktioner

1.1 Styrket sikkerhed omkring samfunds vigtige funktioner
Ministerområder med ansvar for samfundsvigtige funktioner, der i væsentlig grad er it-understøttet, forpligtes til at udarbejde strategier for cyber- og informationssikkerheden samt oprette en decentral cyber- og informationssikkerhedsenhed (DCIS). Strategierne skal i første fase omfatte statsejet kritisk it-infrastruktur og i næste fase også forholde sig til den private, regionale og kommunale sektor.

1.2 De samfundskritiske it-systemer i staten skal være mere sikre
Der indføres nye krav til arbejdet med cyber- og informationssikkerhed for de statslige myndigheder, der har ansvar for samfundskritiske it-systemer. Da en væsentlig del af statens samfundskritiske it-systemer i dag er outsourcet til private leverandører, skal der også ses på muligheden for, at staten om nødvendigt kan overtage it-systemerne, hvis den pågældende leverandør fx rammes af konkurs eller vælger at afvikle sin virksomhed.

1.3 Bedre sikkerhed via ISO-implementering og nye minimumskrav til de statslige myndigheder
Styringen af informationssikkerheden i staten styrkes ved at øge vejledningsindsatsen i forhold til ISO 27001. Samtidig styrkes sikkerheden via videreudvikling af tekniske minimumskrav, som er obligatoriske for alle statslige myndigheder.

1.4 Større fokus på it-sikkerhed ved offentlige it-indkøb og udbud
For at højne cyber- og informationssikkerheden hos de offentlige myndigheder, skal det afdækkes, hvordan it-sikkerhedsaspekter i højere grad kan tænkes ind i de offentlige ramme- og indkøbsaftaler, samt hvorvidt it-sikkerhedsniveauet i aftalerne er tilstrækkelig transparent for myndighederne.

1.5 Fælles tekniske løsninger
Der etableres en række fælles løsninger til styrkelse af sikkerheden i myndighederne, herunder 1) en fællesstatslig sikker DNS-tjeneste, der skal beskytte statslige ansatte mod phishing og malware, 2) et fællesstatsligt sikkerhedsskjold (GovShield), der bl.a. gennem logning og mulighed for udbygning skal hjælpe med at identificere og imødegå cybertrusler hos myndigheder, der ikke er kunder hos Statens It, 3) en effektiv indrapporteringsordning for phishingmails (phishing-portal), så deling af informationer om trusler og indikatorer på kompromitteringer forbedres. Derudover etableres 4) en national it-beredskabsplan, som myndighederne skal tage højde for i deres beredskabsplaner.

1.6 Styrket digital robusthed og digital ledelsesforankring i SMV'erne
Den digitale robusthed i danske SMV'er øges ved at give deres ledelser, medarbejdere og eksisterende rådgivere de bedst mulige forudsætninger for at sikre sig mod den digitale trussel med bl.a. en brugervenlig og interaktiv værktøjskasse og en brobyggerindsats.

1.7 Styrkelse af politiets indsats mod it-kriminalitet
Politiets indsats mod it-kriminalitet styrkes ved at udvide kapaciteten til bagudrettet efterforskning og disruption af it-relateret kriminalitet samt mulighed for, at politiet kan rykke ud til virksomheder ved cyberangreb.

1.8 Øget webpatruljering
Der oprettes i regi af flerårsaftalen for politiet og anklagemyndigheden en webpatruljeenhed i dansk politi, der vil sætte politiet i stand til at forebygge, monitere og efterforske aktiviteter i det digitale rum mhp. at forebygge it-kriminalitet.

1.9 Genopretning af data og samfundskritiske it-systemer i staten
Statslige myndigheder skal have planer for at være i stand til at genoprette data og samfundskritiske it-systemer i tilfælde af skadelige hændelser. Der udarbejdes retningslinjer og vejledninger for anvendelsen af genopretningsplaner og -tests i staten med henblik på, at flere statslige myndigheder tester deres genopretningsplaner. Derudover styrkes indsatsen hos Center for Cybersikkerhed til assistance med genopretning, særligt i sager af betydning for den nationale sikkerhed.

1.10 Hjemmel til at imødegå brede og forstyrrende destruktive cyberangreb
Det undersøges, hvorvidt det er muligt at opbygge kapacitet til at imødegå forstyrrende eller destruktive cyberangreb mod samfundsvigtige funktioner i Danmark gennem tilvejebringelse af hjemmel til at nedtage kompromitterede servere.

1.11 Udvidet analyse af national kritisk it-infrastruktur
Der gennemføres en analyse af de digitale afhængigheder mellem kritisk it-infrastruktur. Analysen vil være et supplement til den igangværende kortlægning af kritisk infrastruktur i Danmark. Formålet er at ruste samfundet til bedre at kunne videreføre samfundsvigtige funktioner, hvis disse rammes af større eller globale cybersikkerhedshændelser.

1.12 Statslig CVD-politik
Der igangsættes et pilotforsøg med en statslig CVD-politik (Coordinated Vulnerability Disclosure). En statslig CVD-politik vil beskrive rammerne for statslige myndigheder til at lade privatpersoner (”hjælpsomme hackere”) identificere og anmelde sårbarheder i it-systemer.

1.13 Styrket akkreditering og tekniske sikkerhedseftersyn
Kapaciteten hos Center for Cybersikkerhed til at foretage akkrediteringer af it-systemer, der behandler klassificerede oplysninger, styrkes. Derudover styrkes kapaciteten til i begrænset omfang at gennemføre tekniske sikkerhedseftersyn for særlige myndigheder samt vejledning og rådgivning af myndigheder herom.

1.14 Fokus på internetudbyderes mulighed for at blokere ondsindede domæner
Det skal undersøges, om internetudbydere som standardydelse kan foretage DNS-blokering af ondsindede domæner. Formålet er at styrke evnen til at identificere, fjerne eller blokere ondsindede domæner og derved opnå en større sikkerhed for internetbrugere i Danmark.

1.15 Alternativ til satellitbaseret tidsstyring
Der udarbejdes en tværsektoriel analyse af behovet for etablering af et eller flere tidsstyringssystemer som alternativ til det eksisterende satellitbaserede tidsstyringssystem. Formålet er at skabe rammerne for etablering af en robust og præcis tidsstyring, som mange nuværende og kommende teknologier i Danmark er afhængige af.

1.16 Styrkelse af udenlandske statsborgeres førstegangsregistrering i CPR
Der igangsættes uddannelsesindsatser for kontrolmedarbejdere hos relevante myndigheder med henblik på at sikre mere valide personoplysninger i CPR-registeret, der er en forudsætning for, at der er tillid til de personoplysninger, som benyttes af mange både offentlige og private instanser.



Øget kompetenceniveau og ledelsesforankring

2.1 Styrket indsats i forhold til viden, awareness og adfærd for topledere og ledere i staten
Der stilles øgede krav til statslige topledere og lederes personlige it-sikkerhed, og kompetenceindsatserne styrkes, så sikkerhed fremover bliver en mere integreret del af ledelsesopgaven.

2.2 Statslige ansatte skal have bedre kompetencer inden for cyber- og informationssikkerhed
Der igangsættes nye kompetenceindsatser, der skal sikre, at alle medarbejdere i staten ved, hvad der kendetegner sikker digital adfærd, og de skal samtidig kunne udøve den i praksis.

2.3 Kompetencer i cybersikkerhed for børn, unge og voksne
Der igangsættes nye indsatser i grundskolen, der skal styrke håndteringen af data i undervisningssektoren gennem vejledning og awarenessindsatser. Dette skal sikre, at børn, unge og voksne er rustet til at begå sig trygt og sikkert digitalt.

2.4 Kompetenceopbygning inden for cyber- og informationssikkerhed gennem de videregående uddannelser
Nye uddannelseselementer på de ordinære uddannelser og en styrket indsats på VVEU skal samlet bidrage til at mindske kompetencegabet inden for cyber- og informationssikkerhed i samfundet.

2.5 Videndeling og cyber- og informationssikkerhed på forsknings- og uddannelsesområdet
Der sættes øget fokus på cybersikkerhed i uddannelsesudbuddet i forsknings- og uddannelsesmiljøerne.

2.6 Styrket informationsindsats over for borgere, myndigheder og virksomheder samt styrkelse af portalen Sikkerdigital.dk
Sikkerdigital.dk skal gøres til Danmarks fælles og autoritative informationsportal for hjælp og vejledning om digital sikkerhed. Dette skal sikre et højt videns- og kompetenceniveau blandt borgere, myndigheder og virksomheder, herunder også store virksomheder. Ved at bygge videre på informationsindsatserne skal der ligeledes rykkes ved adfærden hos de enkelte målgrupper.



Styrkelse af det offentligt-private samarbejde

3.1 Bedre hjælp til borgere og virksomheder via en cyberhotline
Der etableres en hotline i staten, som borgere og virksomheder, herunder også store virksomheder kan henvende sig til for at få hjælp og vejledning om grundlæggende cyber- og informationssikkerhed. Hotlinen skal også kunne give konkret rådgivning om eksempelvis genopretning af data, phishingforsøg og/eller sikring af data til brug for en eventuel efterfølgende politimæssige efterforskning. Hotlinen etableres i et tæt samarbejde med Sikkerdigital.dk.

3.2 Styrket central rådgivningskapacitet
Med initiativet styrkes den centrale rådgivning i Center for Cybersikkerhed på en række områder: 1) styrke den højt specialiserede rådgivningsenhed med fokus på situationsbestemt rådgivning til statslige myndigheder mhp. at løsekonkrete og praktiske udfordringer, 2) øge kapaciteten til at foretage sikkerhedsteknologiske undersøgelser, 3) styrke den analytiske kapacitet ift. cyberkriminalitet og cyberspionage, og 4) styrke kapaciteten i telesektionen mhp. at kunne følge udviklingen af 5G-teknologien og yde rådgivning.

3.3 Etablering af en cybersikkerhedsenhed for SMV'er
For at få en samlet og sammenhængende indsats målrettet SMV'erne, etableres der en cybersikkerhedsenhed, der bl.a. kan samle og dele SMV-relevant viden og erfaringer om hændelser og trusler. Enheden skal bl.a. være med til at facilitere og igangsætte nye offentlig-private initiativer, der skal bidrage til en styrkelse af SMV'ernes cybersikkerhed. Indsatsen tilpasses forskellige typer af SMV'er, da de har varierende modenhed og behov.

3.4 Styrket erfaringsudveksling om og indsigt i cyber- og informationssikkerhedshændelser
Det skal undersøges, hvordan erfaringsudvekslingen og vidensopbygningen på tværs af offentlige og private aktører og mellem sektorer kan styrkes, så relevant viden om konkrete hændelser deles bredest muligt. Der ses også på, hvordan data fra fx Datatilsynet og Rigspolitiet i højere grad kan stilles il rådighed for andre.

3.5 Styrket efterforskningskapacitet til cyberspionage
PET's kapacitet til at efterforske cyberspionage fra statslige aktører styrkes.

3.6 Et styrket værn om statens informationer
Der oprettes en national koordinationsgruppe, der skal styrke samarbejde og koordination mellem myndighederne samt øge rådgivningsindsatsen i forhold til fysisk sikring i statslige myndigheder.

3.7 Styrket sikkerhedstilsyn med systemleverandører og databehandlere
Der udarbejdes en omkostningseffektiv basismodel for tilsynsopgaven med henblik på at styrke og effektivisere myndighedernes tilsyn med databehandlere og systemleverandører inden for informationssikkerhed og databeskyttelse. På baggrund af resultatet kan der gennemføres en konceptafprøvning af tilsynsmodellen på én eller flere it-systemer i staten.



Aktiv deltagelse i den internationale kamp mod cybertruslen

4.1 Styrket bidrag til en regelbaseret international orden
Via en væsentlig styrket indsats i FN og andre norm- og standardsættende organisationer samt gennem øget samarbejde med tech-industrien vil Danmark øge sit bidrag til en regelbaseret international orden i cyberspace og præge spillereglerne på et område, der er afgørende for vores sikkerhed, tryghed og økonomiske fremgang.

4.2 Diplomatiske modsvar
Danmarks kapacitet til at iværksætte og indgå i international koordination af diplomatiske modsvar på cyberangreb såsom attribueringer og sanktioner styrkes, herunder i EU-regi, med henblik på at øge Danmarks afskrækkelses-profil på cyberområdet.

4.3 Styrket kapacitet til at kunne imødegå statslige og ikke statslige aktørers cyberangreb
Der gennemføres en række tiltag mhp. at styrke det nationale cyberforsvar, herunder 1) Cyberanalyseafdelingen hos Center for Cybersikkerhed styrkes med henblik på at øge mulighederne for teknisk attribuering, 2) det skal være muligt at spore påvirkningsaktiviteter i udlandet på sociale medier, 3) der etableres et offensivt cyberforsvar, der kan afdække forberedelser af, varsle om, afskrække og imødegå statslige og ikke statslige aktøres cyberangreb mod Danmark eller vores allierede, 4) den danske vidensopbygning og indflydelse på cyberoperations- og sikkerhedsområdet i NATO styrkes gennem udstationering af medarbejdere og 5) Styrkelse af cybersikkerheden på ambassader gennem ansættelse af designerede tekniske normer, tekniske løsninger samt institutionalisering af vedvarende dedikeret samarbejde på området.

4.4 Styrket afskrækkelse af cyberangreb
Der skal opbygges et aktivt cyberforsvar, der skal sætte os i stand til at forstyrre, vildlede eller standse en modstanders cyberoperationer mod Danmark. Dette indebærer bl.a., at der udsendes en forbindelsesofficer til Europols Joint Cyber Action Task force (J-CAT).

4.5 Styrket kontrol med spredning af cyberprodukter og indefrysning af økonomiske midler
Kontrollen med spredning af cyberprodukter styrkes, så Danmark ikke spreder følsom teknologi, som cyberkriminelle kan få adgang til. Vi skal samtidig hjælpe erhvervslivet til at blive bedre til at indefryse de kriminelles økonomiske midler til brug for hackerangreb.

December 2021

Finansministeriet
Christiansborg Slotsplads 1
1218 København K
Tlf: +45 3392 3333
E-mail: fm@fm.dk

ISBN 978-87-93073-45-6 (digital version)
ISBN 978-87-93073-44-9 (trykt version)

Design: BGRAPHIC
Fotos: Getty Images

Publikationen kan hentes på
fm.dk / regeringen.dk

Finansministeriet
Christiansborg Slotsplads 1
1218 København K
Tlf. +45 3392 3333
E-mail: fm@fm.dk